功能上要求实现实时帐户信息查询。这就使电子商务系统必须在物理上与生产系统要有连接，这对于电子商务系统的安全性提出了更高的要求，必须保证外部网络（INTERNET）用户不能对生产系统构成威胁。为此，需要全方位地制定系统的安全策略。 就整个系统而言，安全性可以分为四个层次 1．网络节点的安全 2．通讯的安全性 3．应用程序的安全性 4．用户的认证管理 其中2、3、4层是通过操作系统和Web服务器软件实现，网络节点的安全性依靠防火墙保证，我们应该首先保证网络节点的安全性。 一、网络节点的安全 1．防火墙 防火墙是在连接Internet和Intranet保证安全最为有效的方法，防火墙能够有效地监视网络的通信信息，并记忆通信状态，从而作出允许/拒绝等正确的判断。通过灵活有效地运用这些功能，制定正确的安全策略，将能提供一个安全、高效的Intranet系统。 2．防火墙安全策略 应给予特别注意的是，防火墙不仅仅是路由器、堡垒主机或任何提供网络安全的设备的组合，它是安全策略的一个部分。安全策略建立了全方位的防御体系来保护机构的信息资源，这种安全策略应包括：规定的网络访问、服务访问、本地和远地的用户认证、拨入和拨出、磁盘和数据加密、病毒防护措施，以及管理制度等。所有有可能受到网络攻击的地方都必须以同样安全级别加以保护。仅设立防火墙系统，而没有全面的安全策略，那么防火墙就形同虚设。 3．安全操作系统 防火墙是基于操作

系统的。如果信息通过操作系统的后门绕过防火墙进入内部网，则防火墙失效。所以，要保证防火墙发挥作用，必须保证操作系统的安全。只有在安全操作系统的基础上，才能充分发挥防火墙的功能。在条件许可的情况下，应考虑将防火墙单独安装在硬件设备上。 二、通讯的安全 1．数据通讯 通讯的安全主要依靠对通信数据的加密来保证。在通讯链路上的数据安全，一定程度上取决于加密的算法和加密的强度。电子商务系统的数据通信主要存在于：（1）客户浏览器端与电子商务WEB服务器端的通讯；（2）电子商务WEB服务器与电子商务数据库服务器的通讯；（3）银行内部网与业务网之间的数据通讯。其中（3）不在本系统的安全策略范围内考虑。 2．安全链路 在客户端浏览器和电子商务WEB服务器之间采用SSL协议建立安全链接，所传递的重要信息都是经过加密的，这在一定程度上保证了数据在传输过程中的安全。目前采用的是浏览器缺省的4O位加密强度，也可以考虑将加密强度增加到128位。 为在浏览器和服务器之间建立安全机制，SSL首先要求服务器向浏览器出示它的证书，证书包括一个公钥，由一家可信证书授权机构（CA中心）签发。浏览器要验征服务器证书的正确性，必须事先安装签发机构提供的基础公共密钥（PKI）。建立SSL链接不需要一定有个人证书，实际上不验证客户的个人证书情况是很多的。验证个人证书是为了验证来访者的合法身份。而单纯的想建立SSL链接时客户只需用户下载该站点的服务器证书（下载可以在访问之前或访问时）。验证此证书是合法的服务器证书通过后利用该证书对称加密算法（RSA）与服务器协商一个对称算法及密钥，然后用此对称算法加密传输的明文。此时浏览器也会

出进入安全状态的提示。 三、应用程序的安全性 即使正确地配置了访问控制规则，要满足计算机系统的安全性也是不充分的，因为编程错误也可能引致攻击。程序错误有以下几种形式：程序员忘记检查传送到程序的入口参数；程序员忘记检查边界条件，特别是处理字符串的内存缓冲时；程序员忘记最小特权的基本原则。整个程序都是在特权模式下运行，而不是只有有限的指令子集在特权模式下运 行，其他的部分只有缩小的许可；程序员从这个特权程序使用范围内建立一个资源，如一个文件和目录。不是显式地设置访问控制（最少许可），程序员认为这个缺省的许可是正确的。百考试题编辑整理 这些缺点都被使用到攻击系统的行为中。不正确地输入参数被用来骗特权程序做一 些它本来不应该做的事情。缓冲溢出攻击就是通过给特权程序输入一个过长的字符串来实现的。程序不检查输入字符串长度。假的输入字符串常常是可执行的命令，特权程序可以执行指令。程序碎块是特别用来增加黑客的特权的或是作为攻击的原因写的。例如，缓冲溢出攻击可以向系统中增加一个用户并赋予这个用户特权。 访问控制系统中没有什么可以检测到这些问题。只有通过监视系统并寻找违反安全策略的行为，才能发现象这些问题一样的错误。 四、用户的认证管理 1．身份认证 电子商务企业用户身份认证可以通过服务器CA证书与IC卡相结合实现的。CA证书用来认证服务器的身份，IC卡用来认证企业用户的身份。个人用户由于没有提供交易功能，所以只采用ID号和密码口令的身份确认机制。 2．CA证书 要在网上确认交易各方的身份以及保证交易的不可否认性，需要一份数字证书进行验证，这份数字证书就是CA证书，它由认证授权中心

（CA中心）发行。CA中心一般是社会公认的可靠组织，它对个人、组织进行审核后，为其发放数字证书，证书分为服务器证书和个人证书。建立SSL安全链接不需要一定有个人证书，实际上不验证客户的个人证书情况是很多的。验证个人证书是为了验证来访者的合法身份。而单纯的想建立SSL链接时客户只需用户下载该站点的服务器证书（下载可以在访问之前或访问时进行）。 五、安全管理 为了确保系统的安全性，除了采用上述技术手段外，还必须建立严格的内部安全机制。 对于所有接触系统的人员，按其职责设定其访问系统的最小权限。 按照分级管理原则，严格管理内部用户帐号和密码，进入系统内部必须通过严格的身份确认，防止非法占用、冒用合法用户帐号和密码。 建立网络安全维护日志，记录与安全性相关的信息及事件，有情况出现时便于跟踪查询。定期检查日志，以便及时发现潜在的安全威胁。 对于重要数据要及时进行备份，且对数据库中存放的数据，数据库系统应视其重要性提供不同级别的数据加密。 安全实际上就是一种风险管理。任何技术手段都不能保证1OO%的安全。但是，安全技术可以降低系统遭到破坏、攻击的风险。决定采用什么安全策略取决于系统的风险要控制在什么程度范围内。F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com